GIGACLOUD

Firewall as a Service у хмарі S-Cloud 2.0

Опис рішення

версія 1.0 2_2021

03022, Україна, м. Київ,
вул. Васильківська, 37-В

+38 (044) 233-71-70
sales@gigacloud.ua

www.gigacloud.ua

Зміст

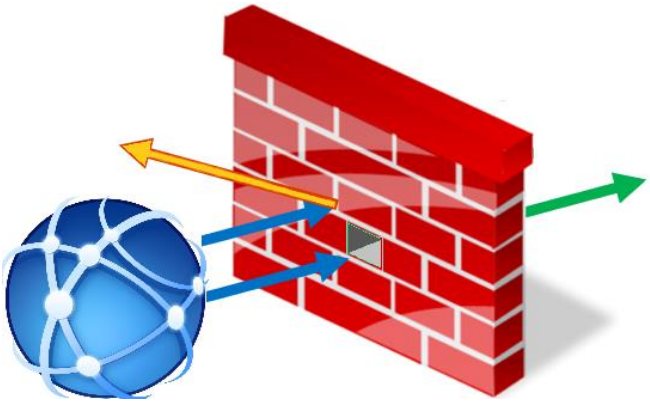
Терміни та визначення 3
Принцип роботи рішення «Firewall as a Service» у хмарі 3
Приклад створення «Firewall as a Service» у хмарі S-Cloud 2.0 4

Терміни та визначення

Хмара, хмарна інфраструктура	Модель надання доступу до розподіленого пулу обчислювальних ресурсів і систем зберігання даних на умовах оренди, з можливістю гнучкої зміни конфігурації та масштабування (за запитом).
ВМ (VM)	Віртуальна машина (virtual machine, віртуальний сервер).
OpenStack	Комплекс проектів вільного програмного забезпечення (ПЗ) з відкритим вихідним кодом, призначений для побудови приватних або публічних обчислювальних хмар та хмарних сховищ. OpenStack побудовано за модульним принципом, де базові модулі комплексу (Compute, Block Storage, Networking, Image Service, Object Storage) керуються за допомогою API/графічної панелі управління Dashboard/інтерфейсу командної строки.
Firewall (або **брандмауер**)	Функція «мережевого екрану» – програмний/програмно-апаратний елемент комп'ютерної мережі, який виконує контроль та фільтрацію трафіку через нього, згідно зі встановленими правилами.

Принцип роботи рішення «Firewall as a Service» у хмарі

Завдяки налаштуванням **Firewall** (або «**брандмауера** – «протипожежної стіни»), дозволений трафік Інтернету пропускається через **екран між мережами** (**WAN** та **LAN**).



Решта з'єднань блокується для захисту локальної мережі від **небажаного зовнішнього трафіку** та зловмисників.

Призначення та принцип роботи **Firewall** в мережах віртуальних та фізичних серверів подібні, тому користування рішенням «**Firewall as a Service**» у S-Cloud 2.0 не повинне викликати складнощів.

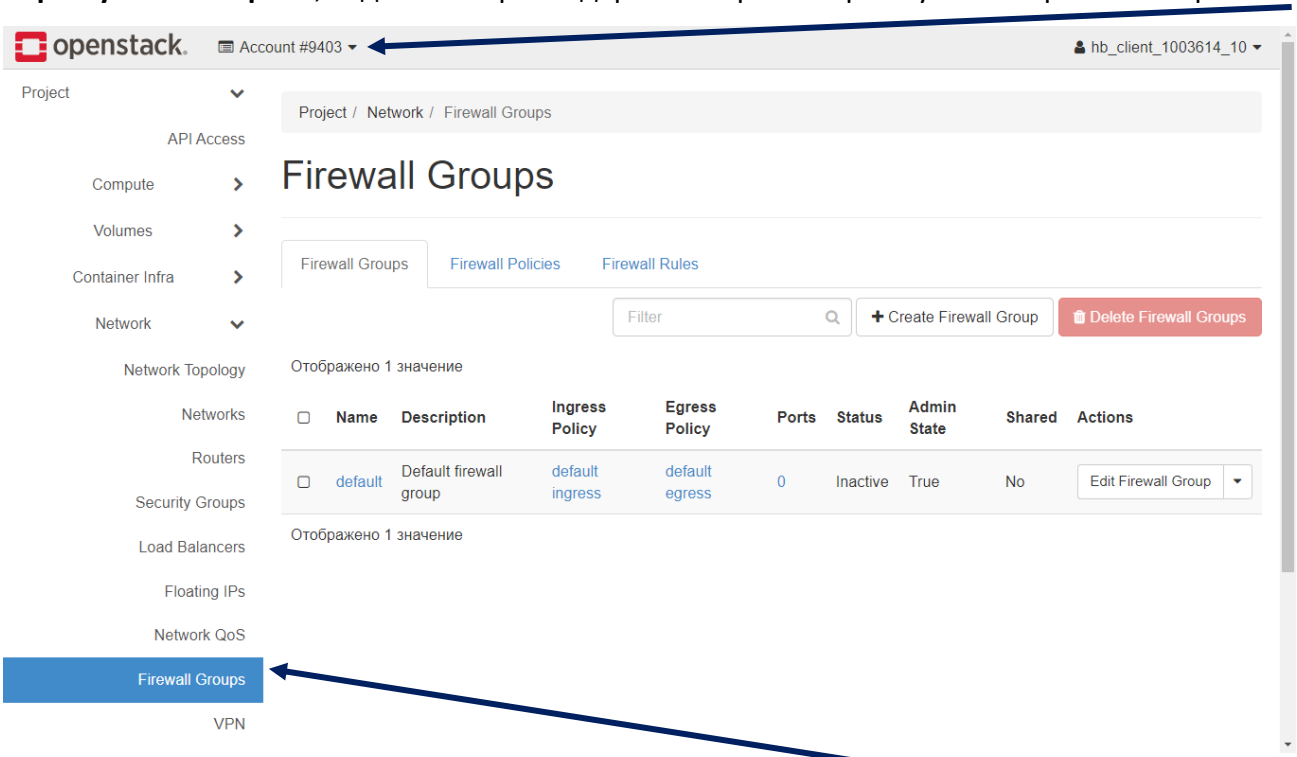
Увага! Порівняння призначення «Firewall as a Service» та «Security Groups»:

- **Рішення «Firewall as a Service»** реалізується **лише на портах віртуального маршрутизатора** проекту користувача та дозволяє **контролювати трафік із зовнішньої мережі** (Інтернет) до внутрішніх ресурсів клієнта (локальних мереж проекту, з підключеними інтерфейсами ВМ);
- **Групи безпеки** («**Project –> Network –> Security Groups**» – налаштування правил фільтрації безпосередньо на ВМ), які забезпечують **контроль взаємних дозволів з'єднання між серверами у локальних мережах проекту**.

Такий **внутрішній захист портів ВМ проти небажаного впливу** з боку інших ВМ проекту (можливо, вже **скомпрометованих внаслідок атаки зловмисників**) підвищує загальний рівень безпеки та працездатності клієнтських сервісів у хмарній інфраструктурі.

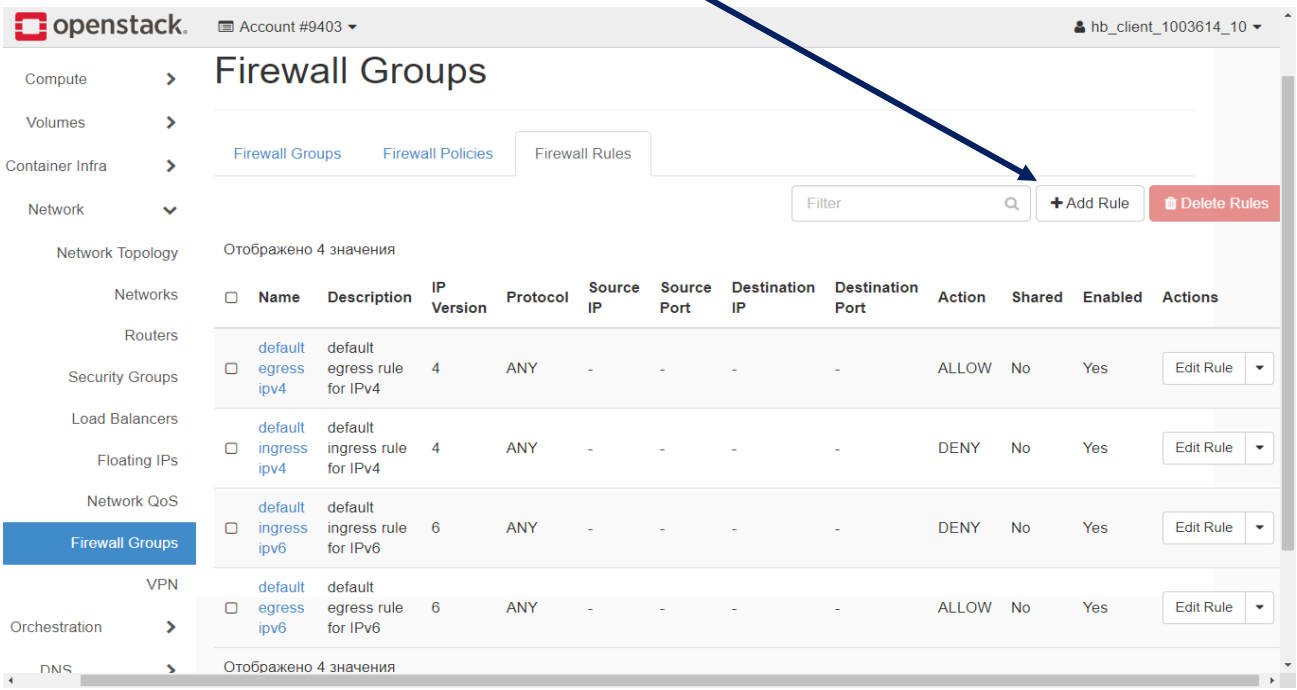
Приклад створення «Firewall as a Service» у хмарі S-Cloud 2.0

Перейдіть до графічної панелі управління Dashboard за вашим URL входу (меню «**Увійти в Horizon**» Клієнтського порталу хмари S-Cloud 2.0). Використовуйте для авторизації **ім'я користувача та пароль**, надані вам провайдером. Оберіть з переліку ваших проектів потрібний.

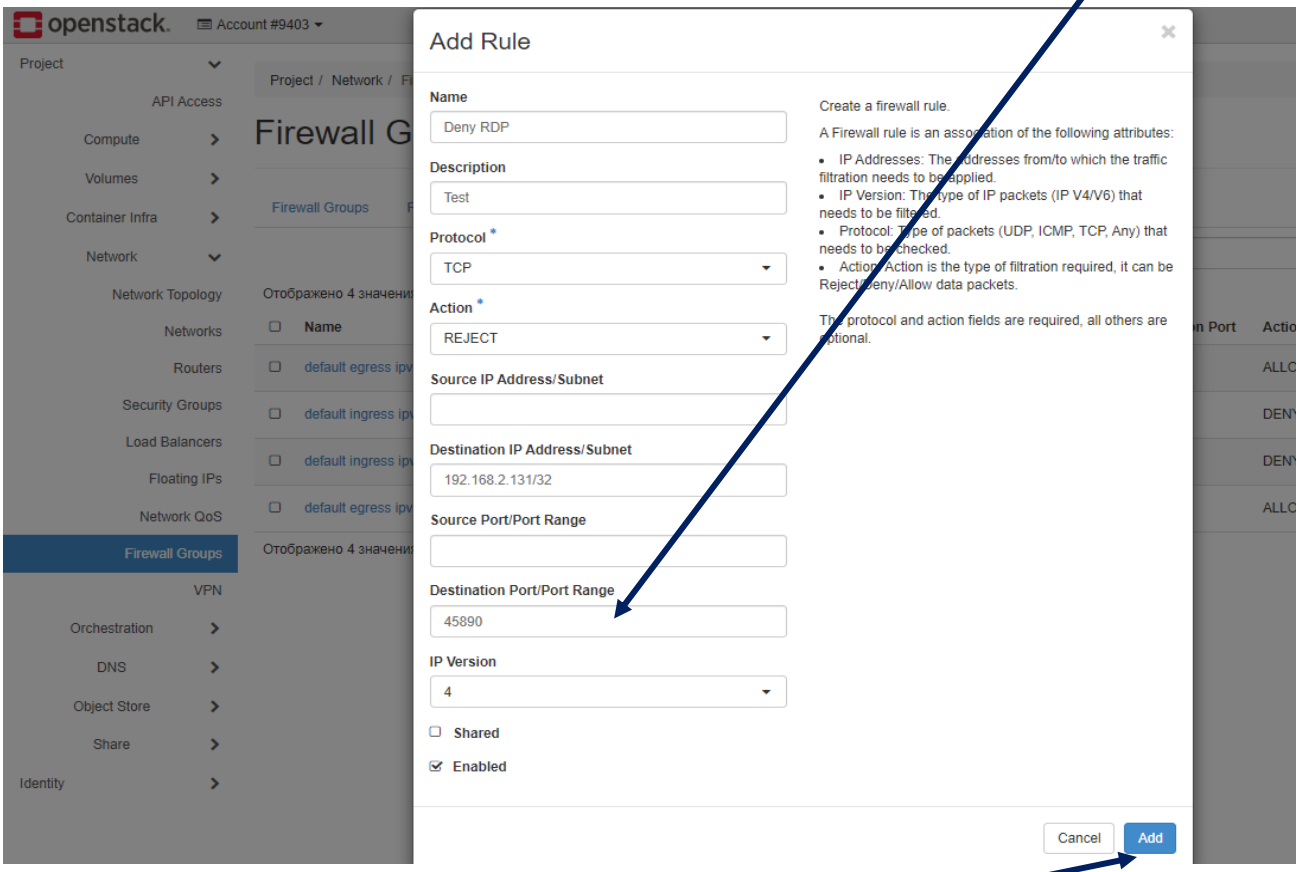


Перейдіть до меню вкладки «**Project –> Network –> Firewall Groups**».

Для створення та налаштування роботи «**Firewall as a Service**», перейдіть до вкладки «**Firewall Rules**» та натисніть екранну кнопку "**Add Rule**":

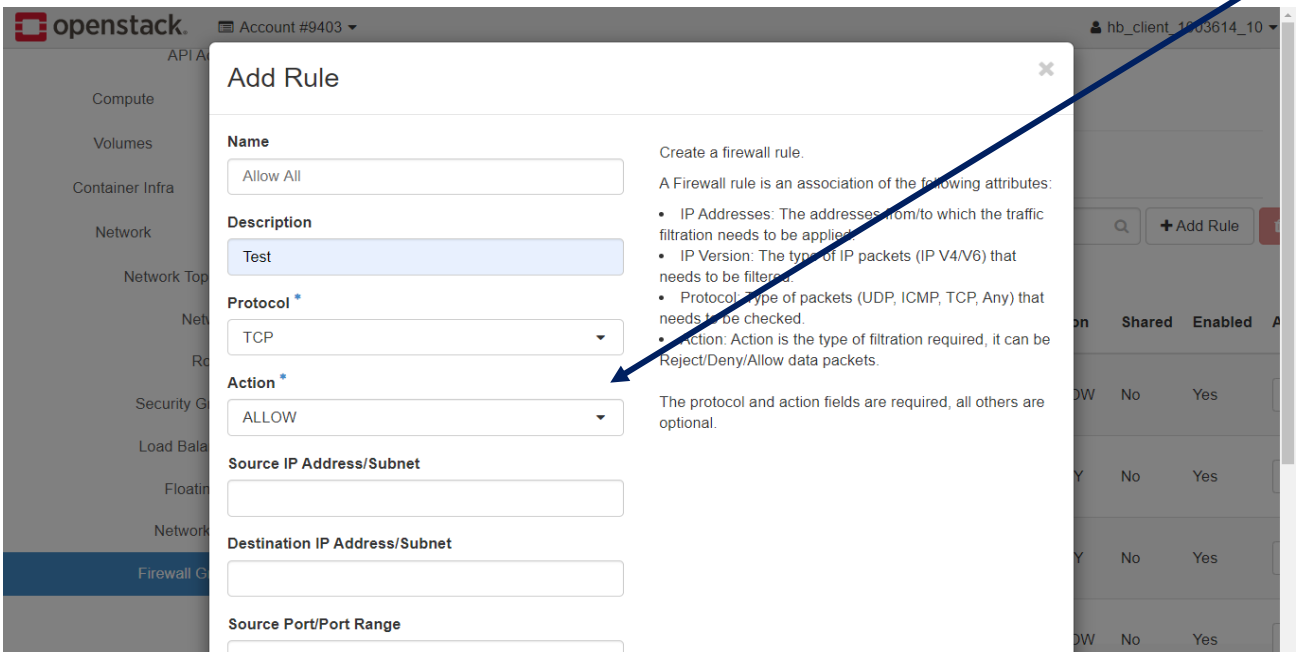


Наприклад, створіть нове правило, що **забороняє** підключення до віддалених робочих столів із використанням протоколу RDP (Remote Desktop Protocol) до одного з серверів проекту (де було налаштовано нестандартне значення порту 45890 замість типового 3389).



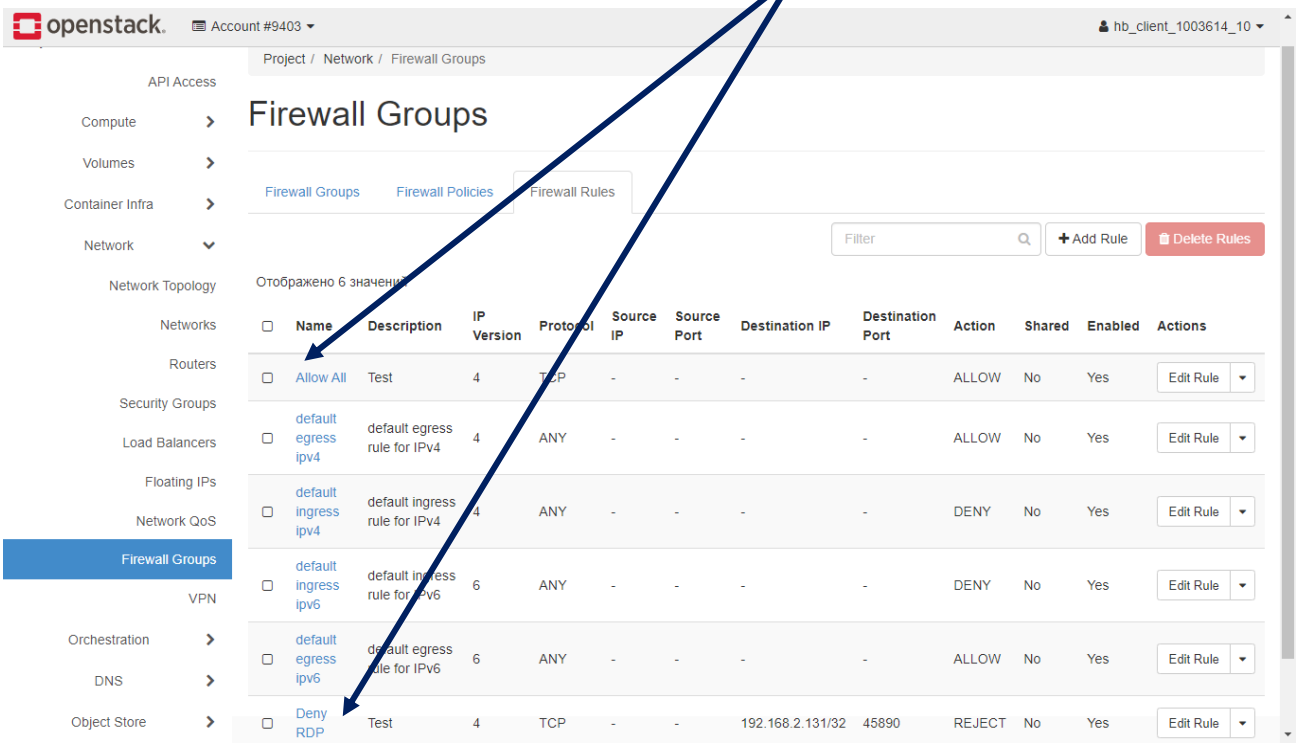
Заповніть необхідні поля форми та натисніть екранну кнопку "**Add**".

Додайте друге правило, що дозволяє весь трафік (оберіть значення в обов'язкових полях):

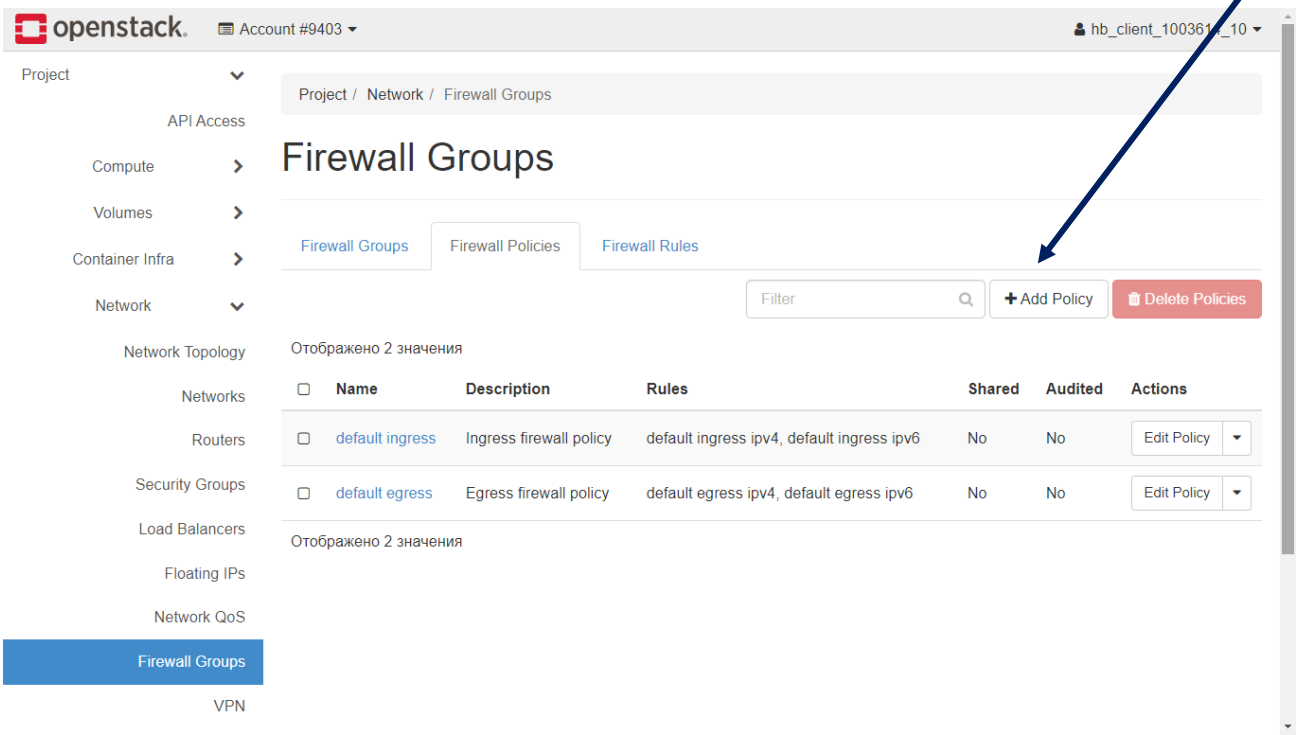


Натисніть екранну кнопку "**Add**".

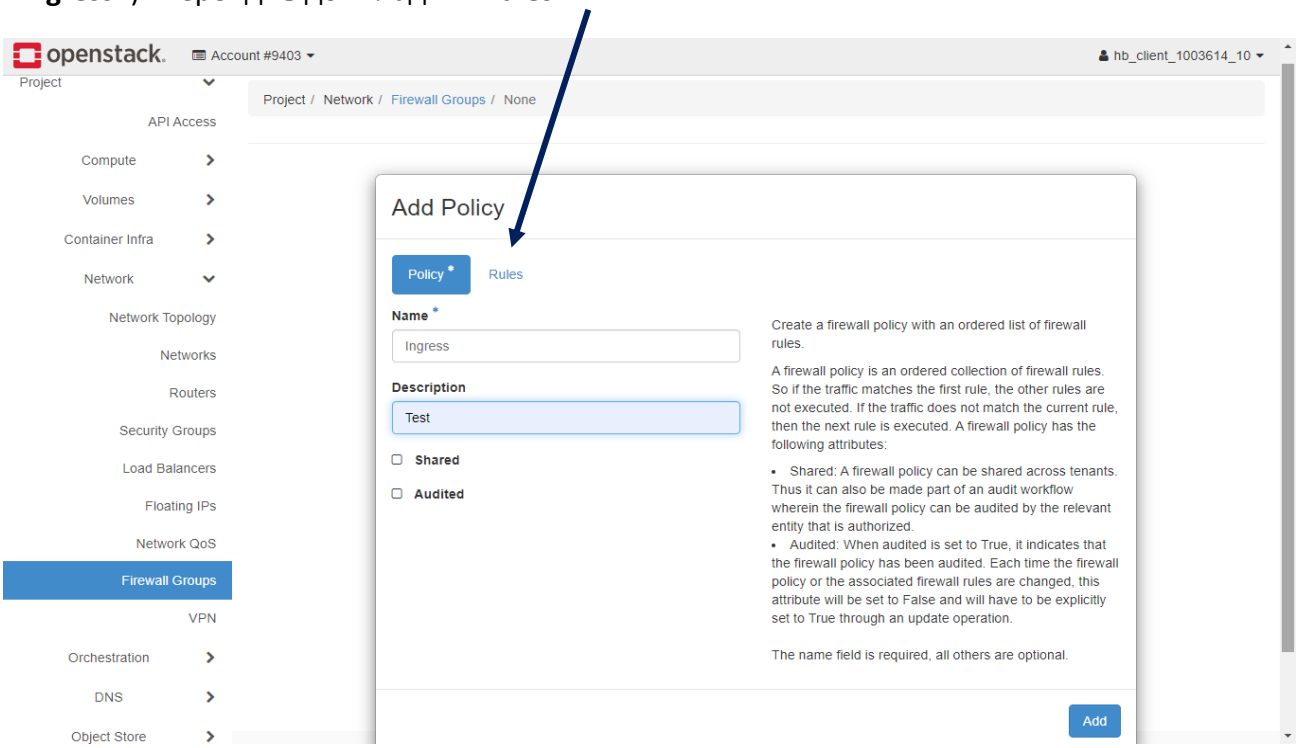
Пересвідчіться, що створені правила додано до переліку:



Створіть політики з використанням щойно створених правил, окремо для вхідного та вихідного трафіків. Перейдіть до вкладки «**Firewall Policies**» та натисніть екранну кнопку "**Add Policy**".

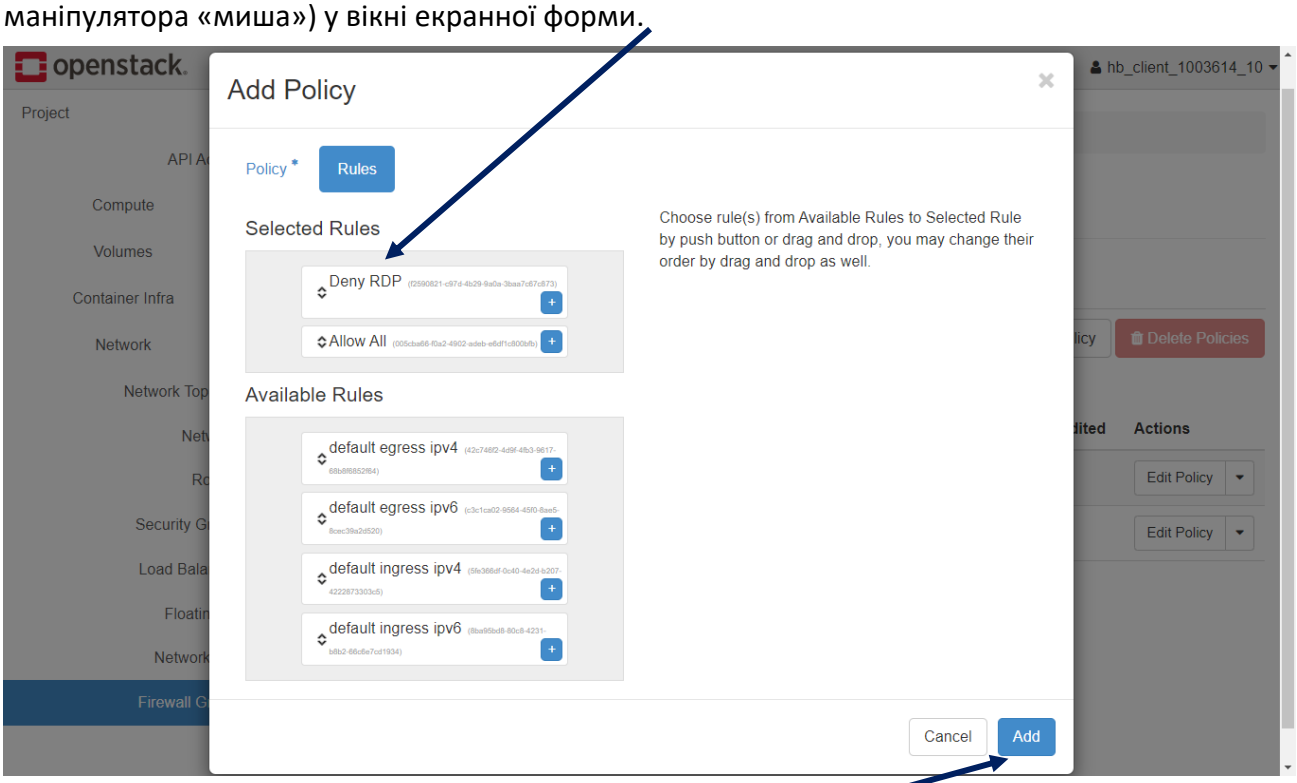


Заповніть обов'язкове поле «**Name**» з найменуванням **політики вхідного трафіку** (наприклад, «**Ingress**») і перейдіть до вкладки «**Rules**»:



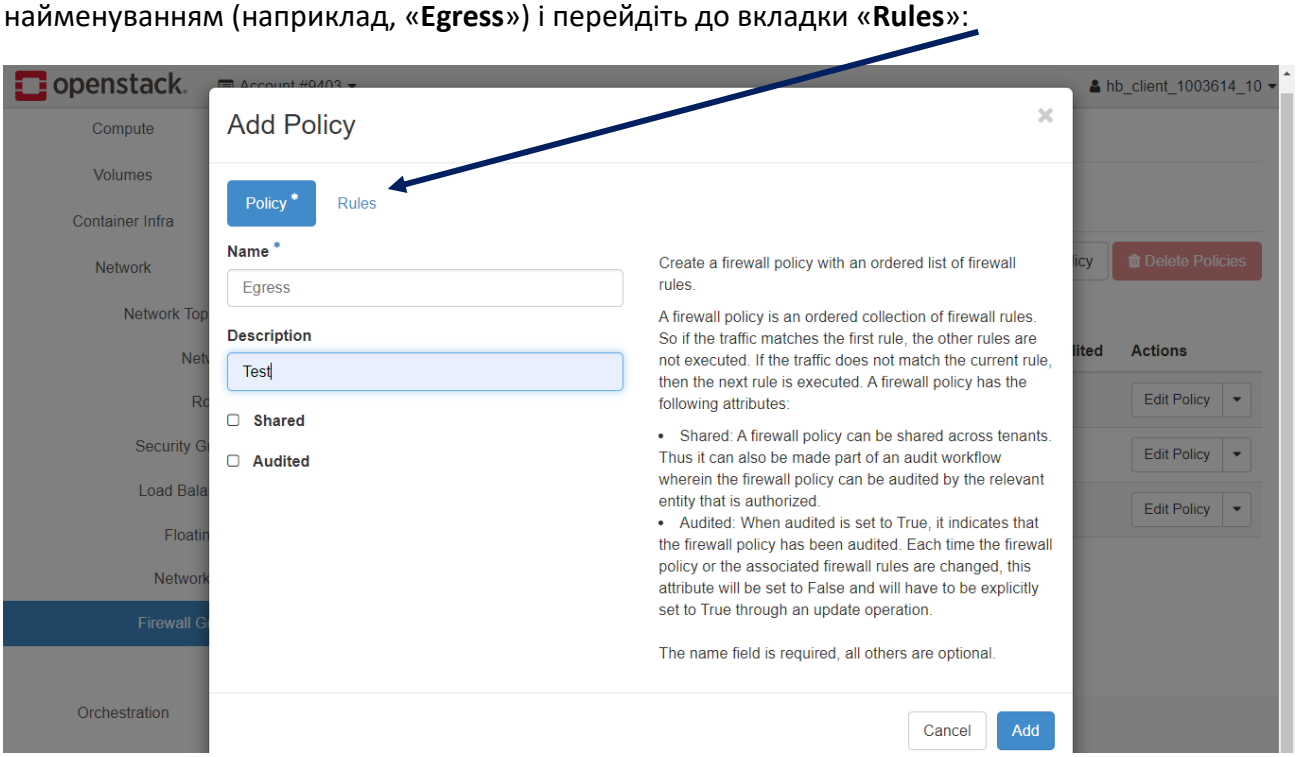
Оберіть щойно створені правила з переліку (**правило заборони повинне бути першим**):

Увага! Послідовність правил у черзі їх виконання – дуже важлива. Для зміни послідовності, ви можете «перетягувати» їх назви вгору/вниз (за допомогою маніпулятора «миша») у вікні екранної форми.

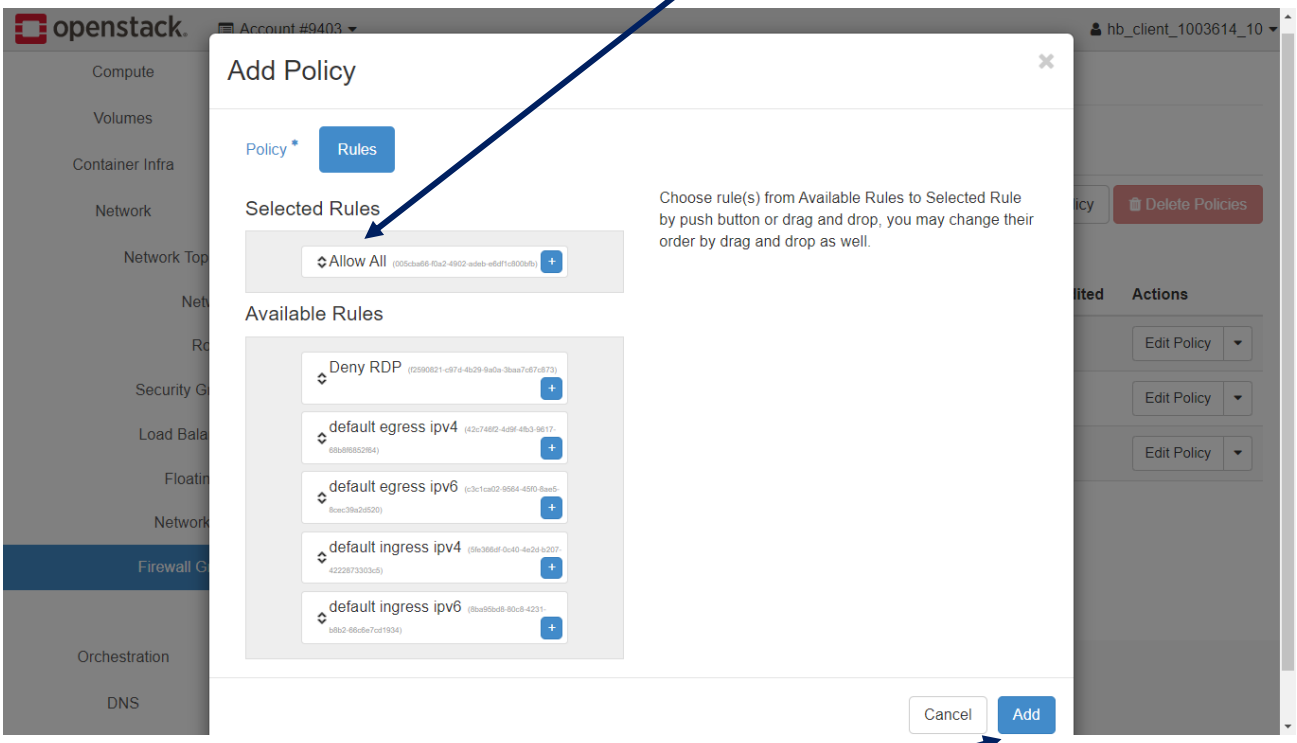


Після завершення редагування, натисніть екранну кнопку "**Add**".

Аналогічно, створіть **політику вихідного трафіку** (заповніть обов'язкове поле «**Name**» з найменуванням (наприклад, «**Egress**») і перейдіть до вкладки «**Rules**»:

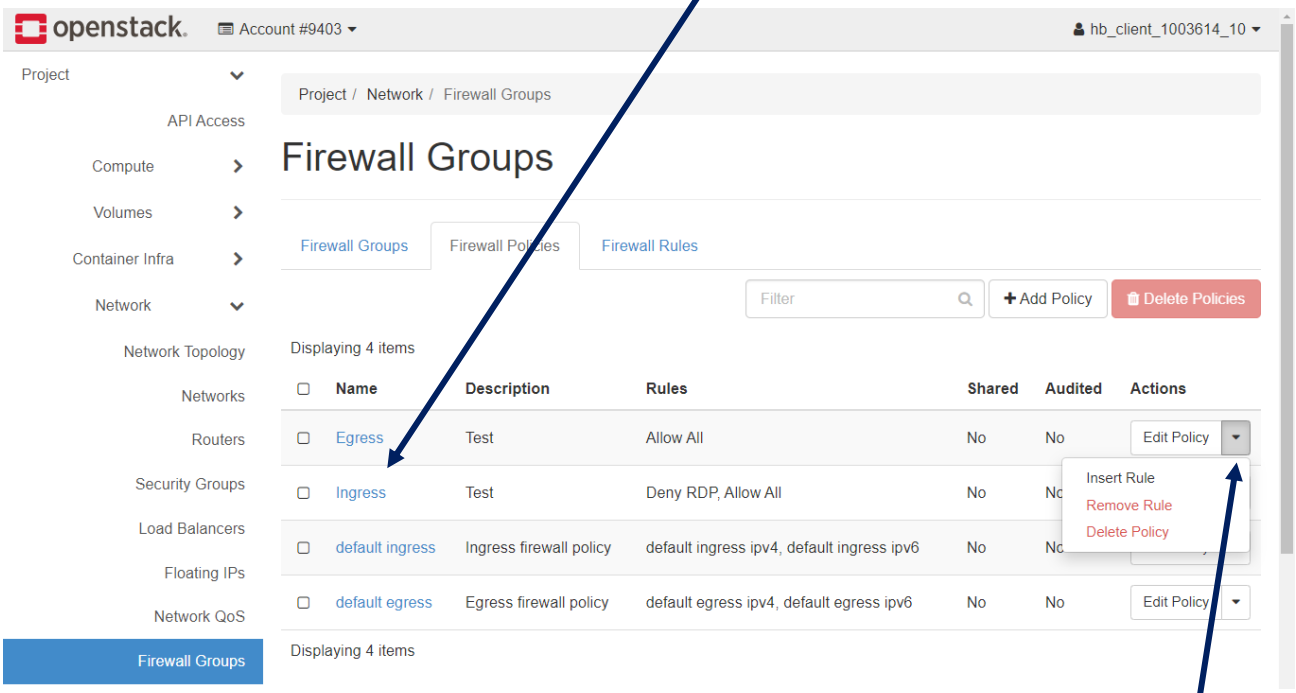


Додайте єдине правило, що дозволяє весь трафік:



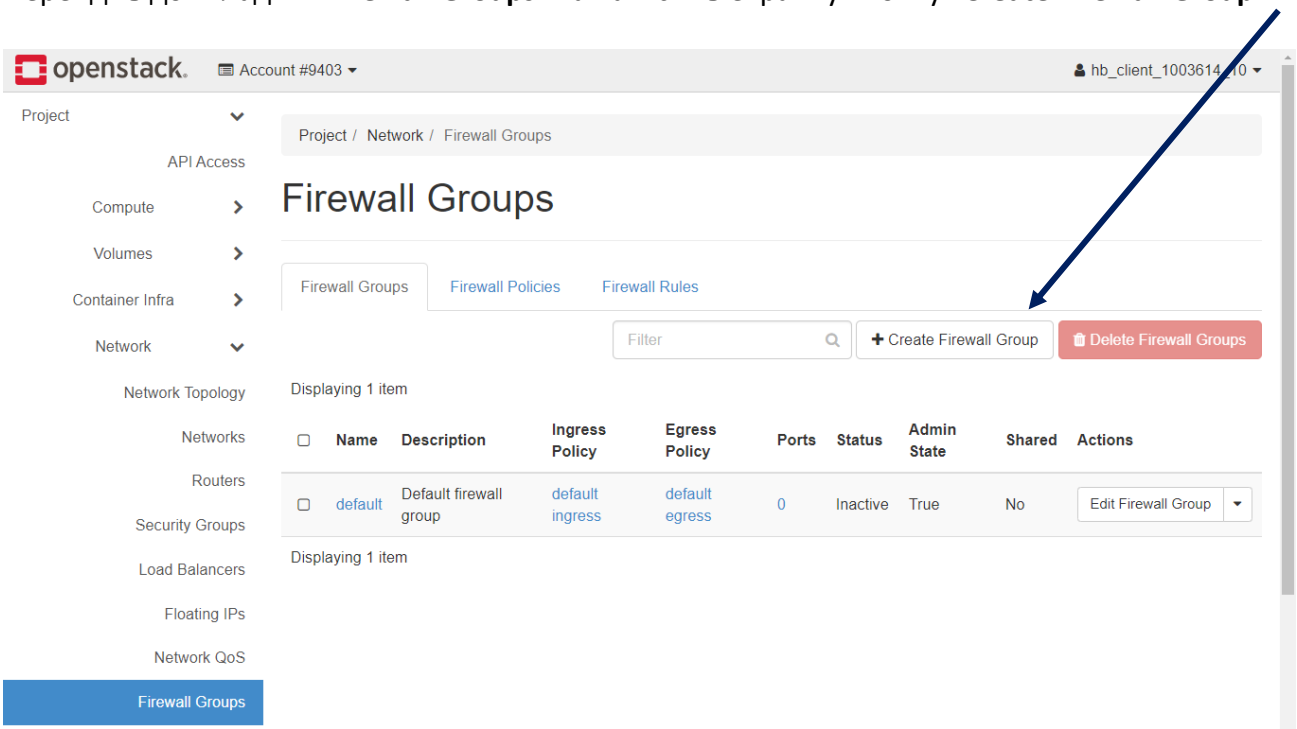
Після завершення редагування, натисніть екранну кнопку "**Add**".

Пересвідчіться, що потрібні вам політики створено:

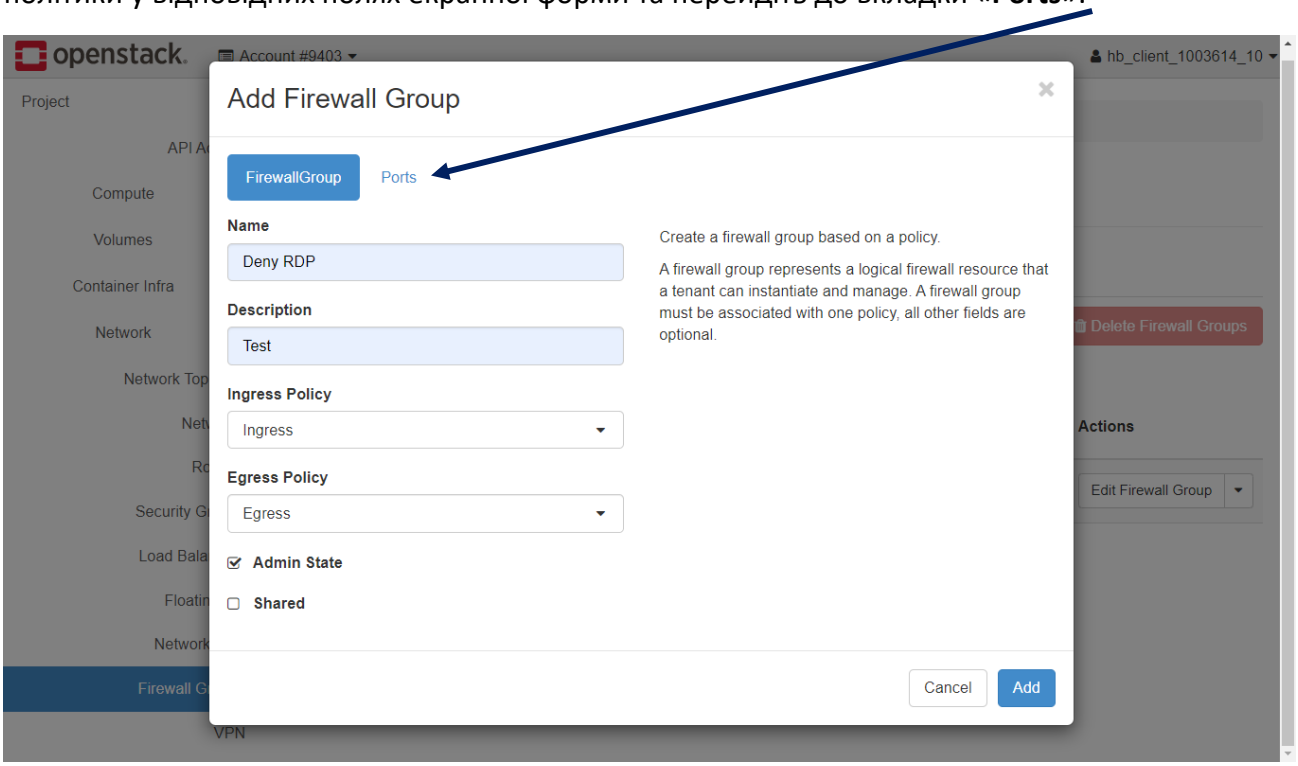


Ви можете змінити найменування та опис політики, користуючись меню «**Edit Policy**».
У разі необхідності, можливо також додати/видалити правила або видалити політику.

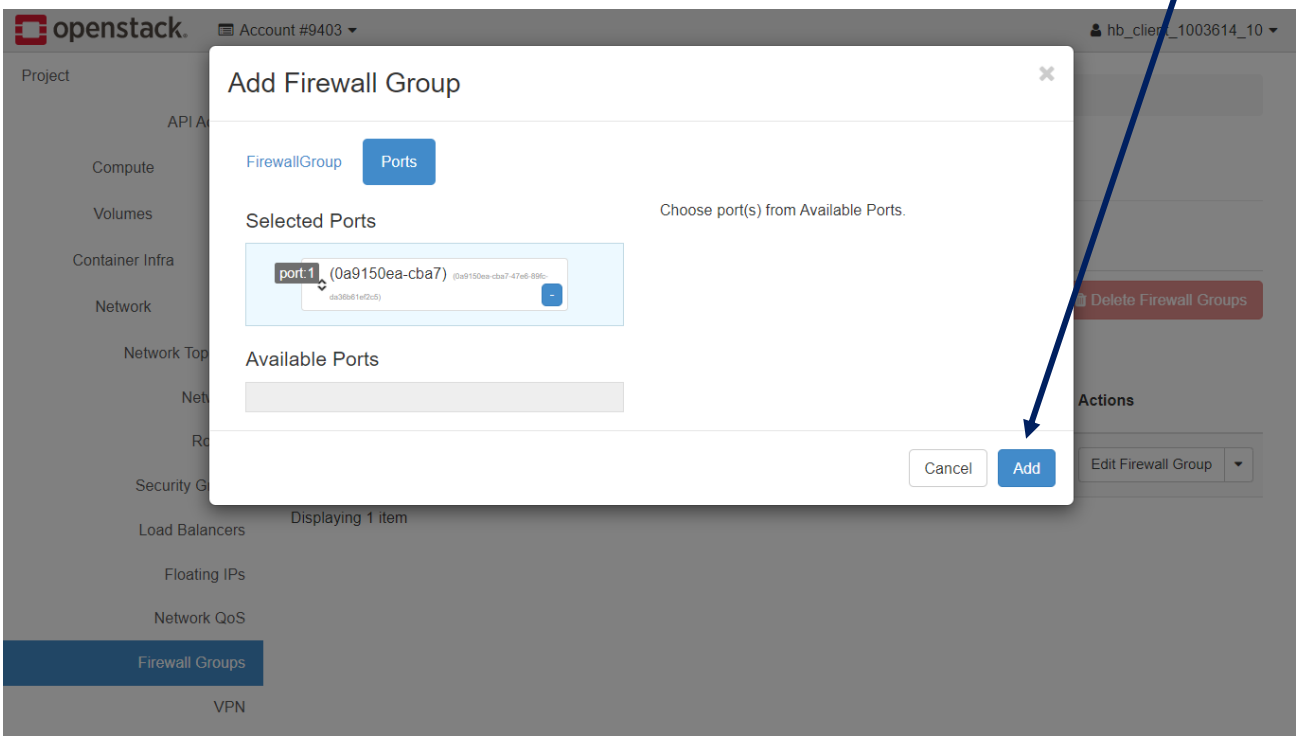
Перейдіть до вкладки «**Firewall Groups**» та натисніть екранну кнопку "**Create Firewall Group**":



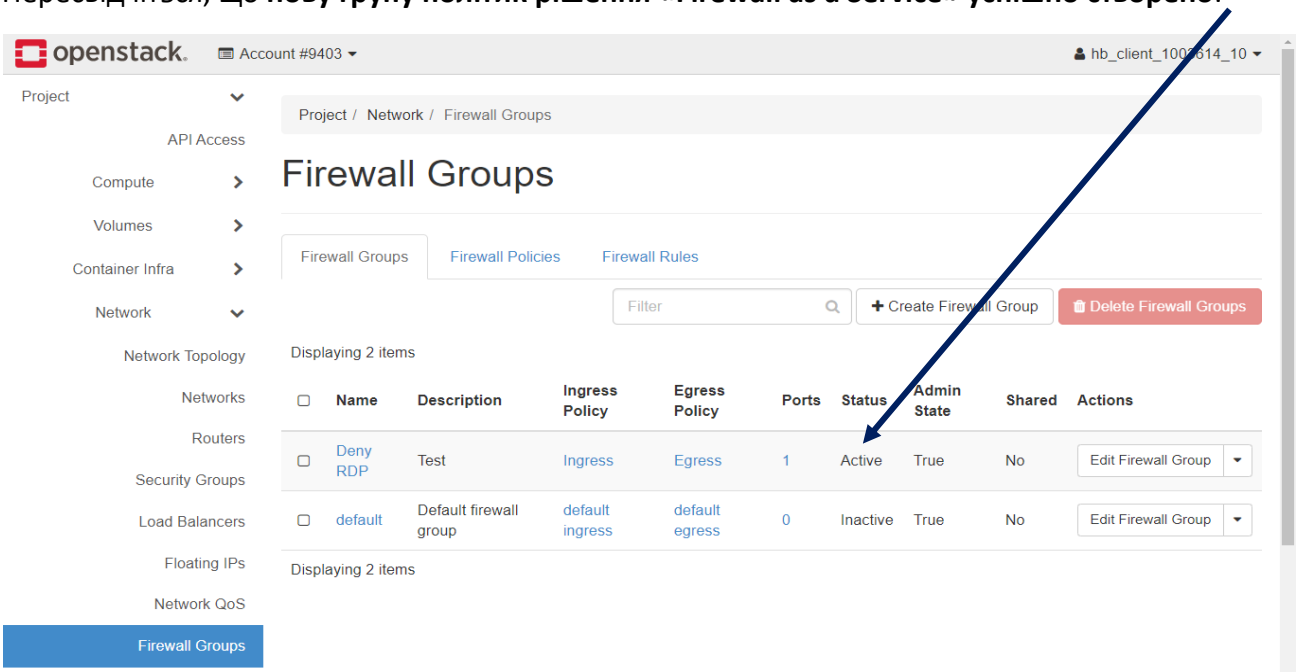
Заповніть поле «**Name**» з найменуванням групи політик файєрвола, оберіть щойно створені політики у відповідних полях екранної форми та перейдіть до вкладки «**Ports**»:



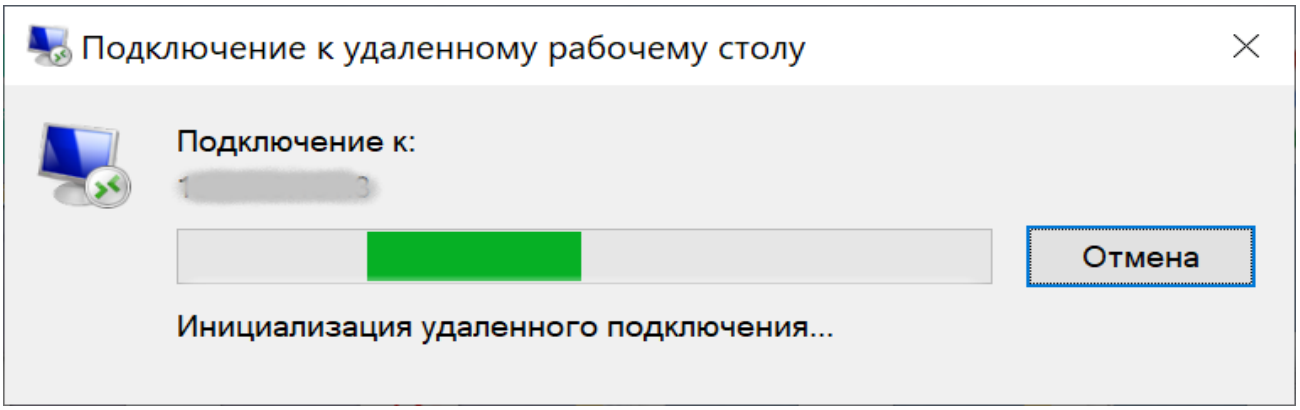
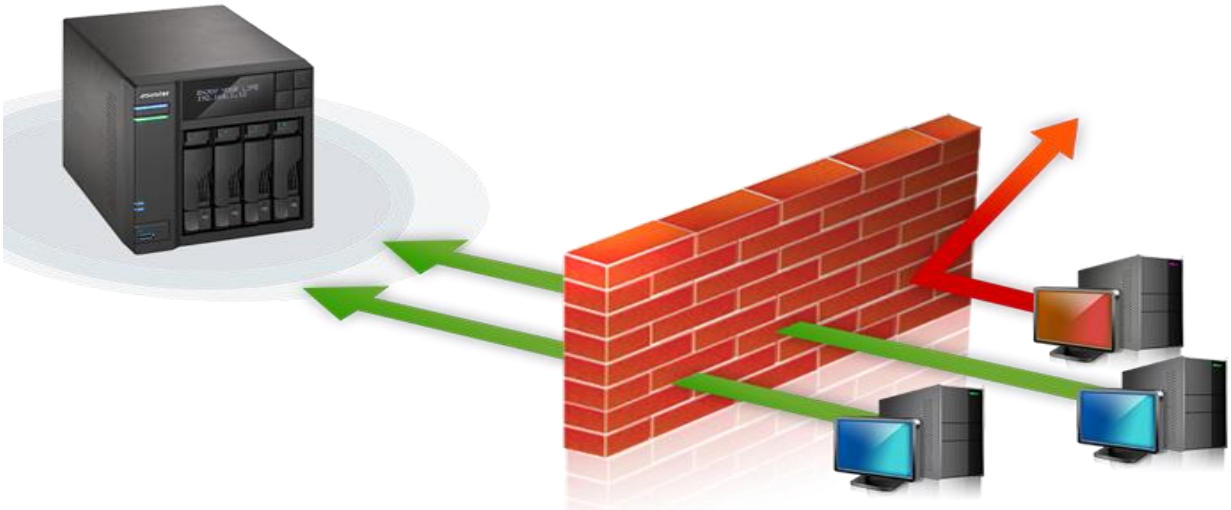
Оберіть порт вашого віртуального маршрутизатора та натисніть екранну кнопку "**Add**".



Пересвідчіться, що **нову групу політик рішення «Firewall as a Service» успішно створено**:



Спробуйте знову підключитися до ВМ (за RDP, зі свого ПК):



Якщо підключення тепер не відбувається - налаштування політик Firewall у вашій хмарній інфраструктурі виконано вірно (**запит на небажане вхідне з'єднання відхилено**).